Upper bounds of a class of imperfect quantum sealing protocols

Guang-Ping He
Department of Physics and Advanced Research Center,
Zhongshan University, Guangzhou 510275, China

The model of the quantum protocols sealing a classical bit is studied. It is shown that there exist upper bounds on its security. For any protocol where the bit can be read correctly with the probability α, and reading the bit can be detected with the probability β, the upper bounds are $\beta \leqslant 1/2$ and $\alpha + \beta \leqslant 9/8$.

PACS numbers: 03.67.Dd, 03.67.Hk, 03.67.-a, 89.70.+c

I. INTRODUCTION

Data sealing is a cryptographic problem between two parties. A sender (Alice) stores some secret data in a certain form, so that any other reader (Bob) can read it without Alice's helping. Meanwhile, if the data has been read, it should be detectable by Alice[1]. A common example of classical data sealing is closing a letter in an envelop with a wafer of molten wax, into which was pressed the distinctive seal of the sender.

Like all other classical cryptographic protocols, it is interesting to find the quantum version of data sealing for better security. Bechmann-Pasquinucci [2] first proposed a protocol which seals a classical bit with a three-qubit state. Singh and Srikanth[3] extended the idea into a many-qubit majority voting scheme, and associated it with secret sharing to improve the security. Chau[4] presented a protocol which seals quantum data with quantum error correcting code. The protocol for sealing a classical string was also proposed[5].

However, as pointed out by the author himself, the protocol in Ref.[2] is insecure against collective measurements. More general, it was further proven[6] that perfect quantum sealing of a classical bit is impossible in principle. If a protocol allows the bit to be perfectly retrievable by the reader, then collective measurements exist which can read the bit without disturbing the corresponding quantum state. It means that Bob can always read the bit without being detected by Alice. In fact, the protocol for sealing quantum data cannot be used for sealing a classical bit either. This is because the quantum states used for encoding the bits 0 and 1 respectively are orthogonal to each other. They can be distinguished by collective measurements without any disturbance too.

Therefore, it is natural to ask whether imperfect quantum sealing of a classical bit is possible. Here "imperfect" means that the sealed bit b is not perfectly retrievable in the protocol. Bob can only read b correctly with the probability $\alpha < 1$, while reading b can be detected with the probability β. Obviously a protocol with $\alpha = 1$ is a perfect one. But if there exists a protocol in which both α and β are less than but very close to 1, it is still very valuable for practical usage.

Nevertheless, in this paper it will be shown that upper bounds exist for α and β. If Bob uses collective measurements instead of the honest operations to read b, then the upper bounds are $\beta \leqslant 1/2$ and $\alpha + \beta \leqslant 9/8$. This result actually bounds the power of practical quantum sealing of a classical bit. In the next section we will establish a general model of imperfect quantum sealing protocols. Basing on the model, the upper bounds will be obtained in Section III. In Section IV some examples of imperfect protocols are studied. The impacts of the result will be discussed in the last section.

II. THE MODEL

First let us establish the model of imperfect quantum sealing protocols, on which the discussion in this paper is based. Note that here and in the following content, when speaking of quantum sealing protocols, we means the protocols for sealing *a classical bit* only, except where noted. The details of the data sealing process is not important to our discussion, but the ending of the protocol generally has the following features:

(1) Bob knows an operation P;

(2) Bob owns a quantum system Ψ (Ψ may not be in the eigenstate of P. Otherwise the protocol becomes a perfect one);

(3) Alice lets Bob know two sets G_0, G_1 ($G_0 \cap G_1 = \emptyset$), such that if he applies P on Ψ and the outcome is $g \in G_0$ ($g \in G_1$), he should take the value of the sealed bit as $b' = 0$ ($b' = 1$); while if $g \notin G_0 \cup G_1$, the sealed bit cannot be identified, i.e. Bob needs to guess b' randomly by himself. Note that since Ψ may not be in the eigenstate of P, the value of b' thus obtained will match Alice's input b with a probability α only;

(4) Alice owns a quantum system Φ entangled with Ψ. And she knows that the initial state of the system $\Phi \otimes \Psi$ is $|\phi \otimes \psi\rangle$;

(5) At any time Alice can access to the entire system $\Phi \otimes \Psi$ and compare its state $|\phi' \otimes \psi'\rangle$ with $|\phi \otimes \psi\rangle$. Thus she can detect whether b has been read with the probability $\beta = 1 - |\langle \phi \otimes \psi | \, \phi' \otimes \psi' \rangle|^2$.

Note that in the protocols previously proposed (e.g. Refs.[2, 3]), Alice does not own the system Φ described above, and the case $g \notin G_0 \cup G_1$ generally will not occur. But to make our result as general as possible so that it may cover other protocols potentially existed, we include

these features in the model. Obviously previous protocols are only the special cases of the model where the entanglement between Φ and Ψ has already collapsed before the end of the protocol, and G_0, G_1 cover all possible outcomes of g.

III. THE UPPER BOUNDS

Let H be the global Hilbert space constructed by all possible states of Ψ. $\{|\hat{e}_i\rangle\}$ denotes a basis of H, which is the eigenvector set of the operation P. It can be divided into three orthogonal subsets $\{\left|\hat{e}_i^{(0)}\right\rangle\}$, $\{\left|\hat{e}_i^{(1)}\right\rangle\}$ and $\{\left|\hat{e}_i^{(2)}\right\rangle\}$, such that $\forall\,|\psi\rangle \in \{\left|\hat{e}_i^{(0)}\right\rangle\}$ ($\forall\,|\psi\rangle \in \{\left|\hat{e}_i^{(1)}\right\rangle\}$), applying P on $|\psi\rangle$ will lead to $b'=0$ ($b'=1$); and $\forall\,|\psi\rangle \in \{\left|\hat{e}_i^{(2)}\right\rangle\}$ will lead to $b'=0$ and $b'=1$ with the equal probability $1/2$. H is consequently divided into three subspaces H_0, H_1 and H_2, whose eigenvector sets are $\{\left|\hat{e}_i^{(0)}\right\rangle\}$, $\{\left|\hat{e}_i^{(1)}\right\rangle\}$ and $\{\left|\hat{e}_i^{(2)}\right\rangle\}$ respectively.

Though the subspaces H_0, H_1 and H_2 are orthogonal to each other, the quantum states used for encoding the bits 0 and 1 respectively need not to be orthogonal in an imperfect quantum sealing protocol. Instead, any state in H could be the state of the system Ψ. That is, the state of Ψ may contain the vectors from different subspaces, so that the states used for encoding 0 and 1 may overlap. In this case, the cheating strategy in the impossibility proof of perfect quantum sealing can not be successful with the probability 1.

However, note that $\{\left|\hat{e}_i^{(0)}\right\rangle\}$, $\{\left|\hat{e}_i^{(1)}\right\rangle\}$ and $\{\left|\hat{e}_i^{(2)}\right\rangle\}$ form a complete basis of H. Let $|\phi_0\otimes\psi_0\rangle$ ($|\phi_1\otimes\psi_1\rangle$) denotes the initial state of $\Phi\otimes\Psi$ when Alice want to seal $b=0$ ($b=1$). It can always be expanded as

$$\begin{aligned}|\phi_b\otimes\psi_b\rangle &= \sqrt{\alpha_b^{(0)}}\sum_i\sqrt{\lambda_{b,i}^{(0)}}\left|\hat{f}_i^{(0)}\right\rangle\left|\hat{e}_i^{(0)}\right\rangle \\ &\quad+\sqrt{\alpha_b^{(1)}}\sum_i\sqrt{\lambda_{b,i}^{(1)}}\left|\hat{f}_i^{(1)}\right\rangle\left|\hat{e}_i^{(1)}\right\rangle \\ &\quad+\sqrt{\alpha_b^{(2)}}\sum_i\sqrt{\lambda_{b,i}^{(2)}}\left|\hat{f}_i^{(2)}\right\rangle\left|\hat{e}_i^{(2)}\right\rangle, \qquad (1)\end{aligned}$$

with $\alpha_b^{(0)}+\alpha_b^{(1)}+\alpha_b^{(2)}=1$, $\sum_i\lambda_{b,i}^{(0)}=\sum_i\lambda_{b,i}^{(1)}=\sum_i\lambda_{b,i}^{(2)}=1$ (sum over all possible i within each corresponding subspace), $b=0,1$. All $\left|\hat{f}_i\right\rangle$ are the vectors describing the state of Φ, which are not required to be orthogonal to each other.

With such initial states, it can be seen that the maximal probability for Bob to read b correctly (i.e. his outcome b' matches Alice's input b) is

$$\alpha=[(\alpha_0^{(0)}+\alpha_0^{(2)}/2)+(\alpha_1^{(1)}+\alpha_1^{(2)}/2)]/2. \qquad (2)$$

Consider a dishonest Bob who does not use P but the following strategy to read b. Define two operators $P_j=\sum_i\left|\hat{e}_i^{(j)}\right\rangle\left\langle\hat{e}_i^{(j)}\right|$ (sum over all possible i within H_j. $j=0,1$), which are the collective measurements projecting the quantum state into the subspaces H_0 and H_1 respectively. Bob randomly chooses to apply either P_0 or P_1 on Ψ with the equal probability $1/2$. If his choice is P_j and Ψ can be projected to the subspace H_j successfully, he takes $b'=j$; else if the projection fails, he always takes $b'=\bar{j}$ without further measurements on the quantum state. That is, he never makes further attempts to distinguish the state between the two subspaces $H_{\bar{j}}$ and H_2. It can be shown that with this strategy, Bob can also reach the maximized α in Eq.(2). Now let us calculate the probability β for the reading to be detected by Alice. There can be four different cases:

(1) *Bob's choice is P_0, and the initial state of $\Phi\otimes\Psi$ is $|\phi\otimes\psi\rangle=|\phi_0\otimes\psi_0\rangle$.* From Eq.(1) it can be seen that Ψ can be projected into H_0 successfully with the probability $\alpha_0^{(0)}$. Meanwhile, $\Phi\otimes\Psi$ collapses to $|\phi'\otimes\psi'\rangle=\sum_i\sqrt{\lambda_{0,i}^{(0)}}\left|\hat{f}_i^{(0)}\right\rangle\left|\hat{e}_i^{(0)}\right\rangle$. It can be viewed as the initial state with the probability $p_{0s}=\left|\langle\phi\otimes\psi|\ \phi'\otimes\psi'\rangle\right|^2=\alpha_0^{(0)}$. Therefore Alice can detect the disturbance of the state with the probability

$$\beta_{0s}=1-p_{0s}=1-\alpha_0^{(0)}. \qquad (3)$$

On the other hand, the projection can also fail with the probability $\alpha_0^{(1)}+\alpha_0^{(2)}$, with $\Phi\otimes\Psi$ collapsing to $|\phi'\otimes\psi'\rangle=(\sqrt{\alpha_0^{(1)}}\sum_i\sqrt{\lambda_{0,i}^{(1)}}\left|\hat{f}_i^{(1)}\right\rangle\left|\hat{e}_i^{(1)}\right\rangle+\sqrt{\alpha_0^{(2)}}\sum_i\sqrt{\lambda_{0,i}^{(2)}}\left|\hat{f}_i^{(2)}\right\rangle\left|\hat{e}_i^{(2)}\right\rangle)/\sqrt{\alpha_0^{(1)}+\alpha_0^{(2)}}$. It can be viewed as the initial state with the probability $p_{0f}=\alpha_0^{(1)}+\alpha_0^{(2)}$. Therefore Alice can detect the disturbance with the probability

$$\beta_{0f}=1-p_{0f}=1-\alpha_0^{(1)}-\alpha_0^{(2)}. \qquad (4)$$

Altogether, in this case reading b can be detected by Alice with the probability

$$\begin{aligned}\beta_0 &= \alpha_0^{(0)}\beta_{0s}+(\alpha_0^{(1)}+\alpha_0^{(2)})\beta_{0f} \\ &= 2\alpha_0^{(0)}(1-\alpha_0^{(0)}). \qquad (5)\end{aligned}$$

Here the condition $\alpha_0^{(0)}+\alpha_0^{(1)}+\alpha_0^{(2)}=1$ is used.

(2) *Bob's choice is P_0, and the initial state of $\Phi\otimes\Psi$ is $|\phi\otimes\psi\rangle=|\phi_1\otimes\psi_1\rangle$.* Similar to the analysis above, in this case reading b can be detected by Alice with the probability

$$\beta_1=2\alpha_1^{(0)}(1-\alpha_1^{(0)}). \qquad (6)$$

(3) *Bob's choice is P_1, and the initial state is $|\phi\otimes\psi\rangle=|\phi_0\otimes\psi_0\rangle$.* Similar to Eq.(5), the detecting probability is

$$\beta_0'=2\alpha_0^{(1)}(1-\alpha_0^{(1)}). \qquad (7)$$

(4) *Bob's choice is* P_1*, and the initial state is* $|\phi\otimes\psi\rangle = |\phi_1\otimes\psi_1\rangle$. Similar to Eq.(6), the detecting probability is

$$\beta_1' = 2\alpha_1^{(1)}(1-\alpha_1^{(1)}). \quad (8)$$

In all, the average probability for Alice to detect the reading is

$$\begin{aligned}\beta &= [\alpha_0^{(0)}(1-\alpha_0^{(0)}) + \alpha_1^{(0)}(1-\alpha_1^{(0)}) \\ &\quad +\alpha_0^{(1)}(1-\alpha_0^{(1)}) + \alpha_1^{(1)}(1-\alpha_1^{(1)})]/2. \quad (9)\end{aligned}$$

The right-hand side of this equation reaches its maximum when $\alpha_0^{(0)} = \alpha_1^{(0)} = \alpha_0^{(1)} = \alpha_1^{(1)} = 1/2$ and $\alpha_0^{(2)} = \alpha_0^{(2)} = 0$. Thus the upper bound for β is

$$\beta \leqslant 1/2. \quad (10)$$

Combining Eqs.(2) and (9), we have

$$\begin{aligned}\alpha+\beta &= [\alpha_0^{(0)}(3/2-\alpha_0^{(0)}) + \alpha_0^{(1)}(1/2-\alpha_0^{(1)}) \\ &\quad +\alpha_1^{(1)}(3/2-\alpha_1^{(1)}) + \alpha_1^{(0)}(1/2-\alpha_1^{(0)}) \\ &\quad +1]/2. \quad (11)\end{aligned}$$

The right-hand side of this equation reaches its maximum when $\alpha_0^{(0)} = \alpha_1^{(1)} = 3/4$, $\alpha_0^{(1)} = \alpha_1^{(0)} = 1/4$ and $\alpha_0^{(2)} = \alpha_0^{(2)} = 0$. Thus we obtain another upper bound

$$\alpha+\beta \leqslant 9/8. \quad (12)$$

IV. EXAMPLES

A. Breaking the majority voting scheme

Here we give an example on how the above cheating strategy is applied to an embodied protocol.

In Ref.[3] a compound scheme was proposed, which embeds a majority voting quantum sealing scheme in a classical secret sharing scheme. As pointed out by the authors, the entire scheme is secure since the secret sharing scheme prevents any single reader from possessing all the qubits to perform collective measurements. Without the secret sharing scheme, as it will be shown below, the majority voting scheme alone is insecure.

The majority voting scheme is defined as follows. To seal a classical bit b, Alice prepares n qubits. fn ($f < 1/2$) qubits called the code qubits are prepared in the state $|b\rangle$. The other $(1-f)n$ qubits called the seal qubits are put randomly in any eigenstate of the diagonal basis $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. To read the bit b, an honest Bob is supposed to measure each qubit in the computational basis $\{|0\rangle, |1\rangle\}$. He takes $b = 0$ (or 1) if more than $n/2$ qubits are found as $|0\rangle$ (or $|1\rangle$). Since $f < 1/2$, we can see that the states encoding 0 and 1 are nonorthogonal to each other. Bob stands a nonzero probability of misreading the bit. Therefore it is an imperfect sealing scheme.

The cheating strategy to this scheme is exactly the one described in the previous section. Let $w(c)$ denote the weight (the number of the bit 1) of a classical binary n-bit string c. The eigenvector set $\{|\hat{e}_i\rangle\}$ in the present case is the computational basis $\{|c\rangle\}$ of the global Hilbert space H, where c runs through all possible classical n-bit strings. Its three orthogonal subsets are defined as $\{\left|\hat{e}_i^{(0)}\right\rangle\} \equiv \{|c\rangle\,|w(c) < n/2\}$, $\{\left|\hat{e}_i^{(1)}\right\rangle\} \equiv \{|c\rangle\,|w(c) > n/2\}$ and $\{\left|\hat{e}_i^{(2)}\right\rangle\} \equiv \{|c\rangle\,|w(c) = n/2\}$. The three subspaces H_0, H_1 and H_2 are consequently defined by these subsets.

For simplicity let us consider the case where n is odd so that $\{\left|\hat{e}_i^{(2)}\right\rangle\} = \emptyset$. Let $|\psi_b\rangle$ be the state of the n-qubit system encoding b. For any $|\psi_b\rangle$ with fn code qubits, we can expand all the $(1-f)n$ seal qubits in the computational basis. Thus $|\psi_b\rangle$ is expanded into $N \equiv 2^{(1-f)n}$ items, of which $M^{(\bar{b})} \equiv \sum_{i=(n+1)/2}^{(1-f)n} \binom{(1-f)n}{i}$ items belong to $\{\left|\hat{e}_i^{(\bar{b})}\right\rangle\}$, while the other $M^{(b)} \equiv N - M^{(\bar{b})}$ items belong to $\{\left|\hat{e}_i^{(b)}\right\rangle\}$. That is

$$\begin{aligned}|\psi_b\rangle &= \sqrt{M^{(b)}/N}\sum_i(\Lambda_i^{(b)}/\sqrt{M^{(b)}})\left|\hat{e}_i^{(b)}\right\rangle \\ &\quad +\sqrt{M^{(\bar{b})}/N}\sum_i(\Lambda_i^{(\bar{b})}/\sqrt{M^{(\bar{b})}})\left|\hat{e}_i^{(\bar{b})}\right\rangle, \quad (13)\end{aligned}$$

where any Λ_i can only be ± 1 or 0, with $\sum_i \Lambda_i^{(b)} = \sqrt{M^{(b)}}$, $\sum_i \Lambda_i^{(\bar{b})} = \sqrt{M^{(\bar{b})}}$. For example, an $n = 5$, $f = 0.4$ state $|11+-+\rangle$ sealing $b = 1$ (the first one in Eq.(1) of Ref.[3]) can be expanded as

$$\begin{aligned}|11+-+\rangle &= (|11000\rangle \\ &\quad +|11001\rangle - |11010\rangle - |11011\rangle \\ &\quad +|11100\rangle + |11101\rangle - |11110\rangle \\ &\quad -|11111\rangle)/\sqrt{8}, \quad (14)\end{aligned}$$

where the first item on the right of the equation belongs to $\{\left|\hat{e}_i^{(0)}\right\rangle\}$, while the other 7 items belong to $\{\left|\hat{e}_i^{(1)}\right\rangle\}$. Obviously when $|\psi_b\rangle$ is measured honestly, b can be read correctly with the probability

$$\alpha = M^{(b)}/N = 1 - \sum_{i=(n+1)/2}^{(1-f)n}\binom{(1-f)n}{i}/2^{(1-f)n}. \quad (15)$$

On the other hand, a dishonest Bob can always use the operator $P_0 = \sum |c\rangle\langle c|$ (sum over all c satisfying $w(c) < n/2$) to perform a collective measurement on $|\psi_b\rangle$. He takes $b = 0$ whenever the projection is successful, else he takes $b = 1$. It can be seen that he can also read b correctly with the above probability α. The probability β for the reading to be detected by Alice can be calculated by repeating the analysis in the previous section. By

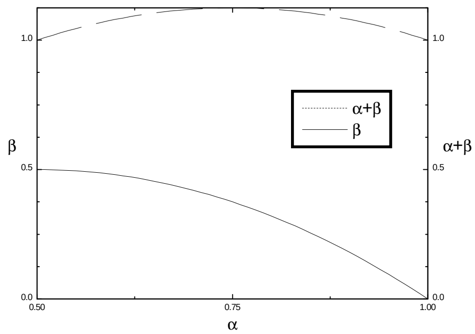

FIG. 1: The security of the majority voting scheme. α is the probability for Bob to read the bit successfully. β is the probability for Alice to detect the reading. The solid line represents β as a function of α. The dashed line represents $\alpha + \beta$ as a function of α.

comparing Eq.(13) with Eq.(1), we find $\alpha_b^{(b)} = M^{(b)}/N$, $\alpha_b^{(\bar{b})} = M^{(\bar{b})}/N$ and $\alpha_b^{(2)} = 0$. Substituting them into Eq.(9) gives

$$\begin{aligned} \beta &= \alpha_b^{(b)}(1-\alpha_b^{(b)}) + \alpha_b^{(\bar{b})}(1-\alpha_b^{(\bar{b})}) \\ &= 2\alpha(1-\alpha) \\ &= 2\left(1 - \sum_{i=(n+1)/2}^{(1-f)n} \binom{(1-f)n}{i} / 2^{(1-f)n}\right) \\ &\quad \cdot \sum_{i=(n+1)/2}^{(1-f)n} \binom{(1-f)n}{i} / 2^{(1-f)n}. \end{aligned} \tag{16}$$

Eqs.(15) and (16) clearly show that in the majority voting scheme, if Alice wants to rise the readability α, the probability β for her to detect the reading will inevitably drop no matter how she chooses n and f. Especially, $\beta \to 0$ when $\alpha \to 1$. This result as well as the value of $\alpha + \beta$ as a function of α are plotted in Fig.1. Thus we see that without being associated with secret sharing, the majority voting scheme alone is insecure against the collective measurement.

B. The scheme that reaches the upper bound $\beta = 1/2$

Eq.(9) indicates that to reach the maximum $\beta = 1/2$, Alice should seal the bit b in the form

$$\begin{aligned} |\phi_b \otimes \psi_b\rangle &= (\sum_i \sqrt{\lambda_{b,i}^{(0)}} \left|\hat{f}_i^{(0)}\right\rangle \left|\hat{e}_i^{(0)}\right\rangle \\ &\quad + \sum_i \sqrt{\lambda_{b,i}^{(1)}} \left|\hat{f}_i^{(1)}\right\rangle \left|\hat{e}_i^{(1)}\right\rangle)/\sqrt{2}. \end{aligned} \tag{17}$$

But clearly such a protocol is useless, since the bit can only be read correctly with the probability $\alpha = 1/2$. Even random guess based on nothing at all can reach such a probability.

C. The scheme that reaches the upper bound $\alpha + \beta = 9/8$

Eq.(11) indicates that to reach the maximum $\alpha + \beta = 9/8$, Alice should seal the bit b in the form

$$\begin{aligned} |\phi_b \otimes \psi_b\rangle &= \frac{\sqrt{3}}{2} \sum_i \sqrt{\lambda_{b,i}^{(b)}} \left|\hat{f}_i^{(b)}\right\rangle \left|\hat{e}_i^{(b)}\right\rangle \\ &\quad + \frac{1}{2} \sum_i \sqrt{\lambda_{b,i}^{(\bar{b})}} \left|\hat{f}_i^{(\bar{b})}\right\rangle \left|\hat{e}_i^{(\bar{b})}\right\rangle. \end{aligned} \tag{18}$$

In this case $\alpha = 3/4$, $\beta = 3/8$. Note that keeping the system Φ (whose state is described by $\left|\hat{f}_i\right\rangle$) at Alice's side is important. Otherwise, consider the simplified version

$$|\psi_b\rangle = \frac{\sqrt{3}}{2} \sum_i \sqrt{\lambda_{b,i}^{(b)}} \left|\hat{e}_i^{(b)}\right\rangle + \frac{1}{2} \sum_i \sqrt{\lambda_{b,i}^{(\bar{b})}} \left|\hat{e}_i^{(\bar{b})}\right\rangle. \tag{19}$$

It cannot reach $\alpha + \beta = 9/8$ if Bob knows that Alice has prepared the states this way. This is because the cheating strategy in the previous section does not require Bob to know the value of α. If he does, he may have other optimal strategies to further reduce β. In the present case, Bob can fake the quantum state with a certain probability after reading it. For example, if he has applied P_0 on Ψ and the projection fails, he knows that the state has collapsed to $\sum_i \sqrt{\lambda_{b,i}^{(1)}} \left|\hat{e}_i^{(1)}\right\rangle$. Since he knows α, he can use a unitary transformation to shift the state into $\sqrt{1-\alpha} \sum_i \sqrt{1/N_0} \left|\hat{e}_i^{(0)}\right\rangle + \sqrt{\alpha} \sum_i \sqrt{\lambda_{b,i}^{(1)}} \left|\hat{e}_i^{(1)}\right\rangle$ (N_0 is the dimensionality of H_0). This generally increases his chance to survive through Alice's detection. Therefore the value of $\alpha + \beta$ in this protocol will be further reduced. This is also true for the majority voting scheme discussed in the section IV.A. If Bob knows f he knows α from Eq.(15), so that he can further reduce β. But if there is a system Φ at Alice's side, it cannot be faked by Bob. Then changing the state at his own side alone will be useless and the upperbound could be reached.

V. DISCUSSION AND CONCLUSION

The upper bounds $\beta \leqslant 1/2$ and $\alpha + \beta \leqslant 9/8$ found in this paper can be seen as an extension of the impossibility proof of perfect quantum sealing of a classical bit[6]. The latter can be seen as the special case where $\alpha = 1$. Eq.(2) shows that $\alpha = 1$ means $\alpha_0^{(0)} = \alpha_1^{(1)} = 1$ and $\alpha_0^{(1)} = \alpha_0^{(2)} = \alpha_1^{(0)} = \alpha_1^{(2)} = 0$. Substituting these values into Eq.(9) immediately gives $\beta = 0$.

Due to the existence of these upper bounds, quantum sealing seems to be far from practical usage, unless we can find a protocol that cannot be covered by the model proposed in Section II. However, so far there still has no sign on the existence of such a protocol. Luckily, as

mentioned above, our model is limited to the protocols which seal a single classical bit. The protocol which seals a classical string[5] is not covered and can be secure.

Very recently, the insecurity of quantum sealing was also studied by Chau[7], in which a more detailed model of quantum sealing ($\{g \notin G_0 \cup G_1\} = \emptyset$ and Bob knows α) was analyzed with a different approach. The result $\beta \leqslant 1/2$ was also obtained, which consists with the finding in the present paper.

I would like to thank Helle Bechmann-Pasquinucci, R. Srikanth and Hoi-Fung Chau for their useful discussions.

---

[1] In fact, in the original proposal of Ref.[2], the detection was suggested to be performed by another verifier authorized by Alice. For simplicity without loss of generality, we may assume that the verifier can get as much information as he needs from Alice, so that he can maximize the successful probability of the detection. Therefore the verifier can be taken as Alice herself.

[2] H. Bechmann-Pasquinucci, Int. J. Quant. Inform. **1**, 217 (2003).
[3] S. K. Singh, R. Srikanth, quant-ph/0410017. To appear in Physica Scripta.
[4] H. F. Chau, quant-ph/0308146.
[5] G. P. He, quant-ph/0502091v2.
[6] H. Bechmann-Pasquinucci, G. M. D'Ariano, C. Macchiavello, quant-ph/0501073. Accepted for publication in Int. J. Quant. Inform.
[7] H. F. Chau, quant-ph/0503031.